Performance Analysis of Key Management Schemes in Wireless Sensor Network Using Analytic Hierarchy Process

Article · November 2011

DOI: 10.1109/TrustCom.2011.243

CITATIONS
3

READS
31

4 authors, including:

Yoshiaki Hori
Saga University
109 PUBLICATIONS **453** CITATIONS

SEE PROFILE

Kouichi Sakurai
Kyushu University
506 PUBLICATIONS **2,769** CITATIONS

SEE PROFILE

Performance Analysis of Key Management Schemes in Wireless Sensor Network Using Analytic Hierarchy Process

Na Ruan*, Yizhi Ren†,Yoshiaki Hori*, Kouichi Sakurai*
* Department of Informatics, Kyushu University, Fukuoka, Japan
† School of Software Engineering, Hangzhou Dianzi University, China
Email: ruanna@itslab.inf.kyushu-u.ac.jp, renyizhi@gmail.com {hori,sakurai}@inf.kyushu-u.ac.jp

***Abstract*—To achieve security in wireless sensor networks (WSNs), key management is one of the most challenging issues in design of WSN due to resource-constrained sensor nodes. Various key management schemes (KMs) have been proposed to enable encryption and authentication in WSN for different application scenarios. According to different requirements, it is important to select the trustworthy KMs in a WSN for setting up a fully appropriate WSN mechanism. An Analytic Hierarchy Process (AHP)-aided method helping with the complex decision has been presented in our previous work. Our purpose in this paper is to do performance analysis of KMs in WSN using our previous AHP-aided method. We analyze the characters of abundance KMs intuitively. The following five performance criteria are considered: *scalability, key connectivity, resilience, storage overhead* and *communication overhead*. As all permutations of five performance criteria include 120 types' situations, experimental analyses on 43 KMs for the optimum selection are presented.**

***Index Terms*—Analytic Hierarchy Process, Experimental analysis, Key management schemes, Optimum selection, Wireless sensor network**

I. Introduction

A. Background

The application area of WSN includes military sensing and tracking, environmental monitoring, patient monitoring and smart environment. In the situation that a sensor node is installed in a dangerous and untrusted area, we should take more concern about its security. Thus, WSN security is a prerequisite for wider use [1].The communication channels between any pair of nodes inside WSN must be protected to avoid attacks from external parties. Such protection, in terms of confidentiality, integrity and authentication, is provided by some security primitives. A key management scheme (KM) is an important security primitive for WSN. The task of generating and distributing those keys has to be done by a global key management system [2]. But WSN is energy limited and not able to support high overhead KM. For this trade-off problem, to design a trustworthy KM in WSN is necessary work.

B. Related Works

In recent years, there has been a significant progress in key management of WSN. Researchers have proposed a number of KMs in WSN. Such as, random pre-distribution key management scheme based on key-pool [7], pre-distribution key management scheme based on polynomial [8], pre-distribution key management scheme based on block design [9], pre-distribution key management scheme based on position [10] and pre-distribution key management scheme based on matrix [11], etc.

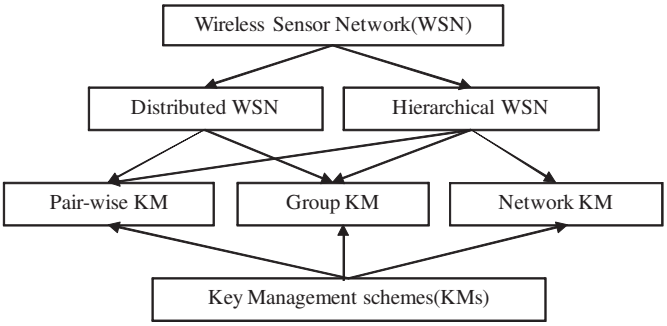


Fig. 1. Classification of Key Management schemes in WSN

Based on the network architecture (hierarchical WSN and distributed WSN), KMs in WSN can be categorized into several types. In Hierarchical WSN (HWSN), data flows are divided into three parts: pair-wise (unicast) among pairs of sensor nodes and from sensor nodes to base station; group-wise (multicast) within a cluster of sensor nodes; network-wise (broadcast) from base stations to sensor nodes. In Distributed WSN (DWSN), data flow is similar to that in HWSN with a difference that network-wise (broadcast) messages can be sent by every sensor nodes. KMs in WSN is organized in distributed or hierarchical structures as shown in Fig. 1 [2] [3].

The Analytical Hierarchy Process (AHP) method is a decision approach designed to aid in the solution of complex multiple criteria problems in a number of application domains [4]. The AHP method has particular application in group decision making. It is used around the world in a wide variety of decision situations, in fields such as government, business, industry, healthcare, and education. A few researchers have used AHP with complex decision. Such as, Hwang et al. [5] employs AHP method in guiding information security policy decision making. It pave the way to use the application of AHP

as a method to develop information security decision model for information security policy.

C. Challenging Issues

Existing KMs in WSN satisfy the special different security requirements. They have their own advantages and disadvantages. Many KMs have been designed to address the tradeoff between limited computational resources and security requirements. It is not easy to determine whether the selected KM scheme is optimum scheme for assumed scenario. Each of the KMs can be suitable for different needs. Recent research works is mainly related to produce an efficient system to evaluate these key management schemes.

To select the most proper KM from large amount of existing schemes is not an easy issue. Many researchers proposed the evaluation index for KMs using the qualitative analysis [2]. Unfortunately, few of these proposals consider the node replication attacks and robustness. Their proposals fail to address all the criteria that a KM should satisfy. Despite the utmost importance of a generic evaluation method for these existing KMs, it is surprising that we find almost nothing in literature on this subject. We present an AHP-aided method for KMs evaluation in WSN [3] for updating. We find there are some interesting characteristics in our previous evaluation results. This pushes us to do further performance analysis among amount KMs in WSN based on our previous AHP-aided work.

D. Our Contribution

In this paper, we propose performance analysis on almost all current existing KMs using AHP. Experimental results will help to obtain the characters of KMs in WSN intuitively. For example, the scores of KMs for DWSN are higher than KMs for HWSN under the Network scenario A which requires distributed scenario. The contributions of our paper can be summarized as follows:

1) We classify six typical KMs and make comparison among the tradeoff in those schemes and show that our method can be helpful in a complicated WSN environment according to the quantitative analysis results.
2) We provide experimental analysis on almost all current existing KMs. We analysis 43 KMs. Our analysis based on the all permutation of 5 criteria. There are 120 types' situations of the importance scale among the 5 criteria.
3) Via our experimental analysis, there are some generic conclusions of features for these existed KMs.

II. Preliminaries

In this section, we introduce our previous AHP-aided method [3]. In our previous work, we propose a generic method to evaluate KMs. The generic method is an AHP-aided method which can help us to select optimum scheme quantitatively according to different network scenario requirements. We present the principle of the method first and then show a case study for extended explanation.

A. Brief reviews of AHP-aided method

There are three steps for considering decision problems: constructing hierarchies, comparative judgment and synthesis of priorities. After constructing hierarchies, both the importance preference of each criteria and the importance preference of each scheme are given as two inputs. With the two inputs, the framework of AHP-aided method [3] for choosing the most suitable key management scheme when considering the preference criteria is presented in Fig.2. Both pair-wise comparison Matrix A for network scenario and series of pair-wise comparison Matrix B for criteria are constructed based on pair-wise element compare. Both consistency check and calculation of weight coefficient value for each scheme are followed for judgement. The synthesis of priorities is gotten during final decision.

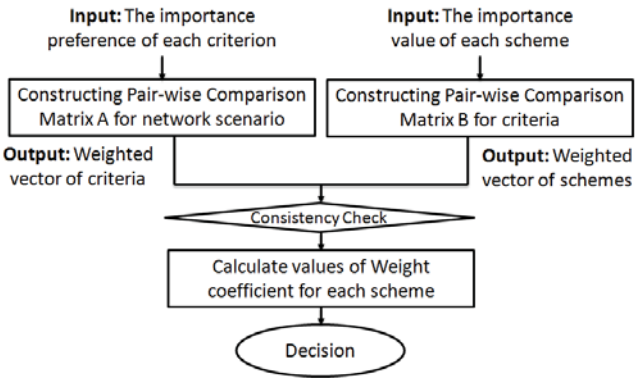


Fig. 2. Hierarchies of our previous proposal

Detailed elaboration on synthesis of priorities are as follows, n: the order of matrix; RI: the average random index; CR: the consistency ratio; CI: the consistency index; λ: the maximum eigenvalue [4]. The inputs are five criteria and six alternative KMs in our former proposed method. Consistency check for 5-order matrix and 6-order matrix should be presented. As when n equals to 5, RI is 1.11 correspondingly. Because the matrix should be validated to pass the consistency check, $CR = CI/RI$ need to be smaller than 0.1 [3]. Thus, CI needs to satisfy that $CI < 0.1 \times 0.11 = 0.011$. Furthermore, as $CI = (\lambda - n)/(n-1) = (\lambda - 5)/4$ and $CI < 0.011$, the 5-order matrix will pass the consistency check when λ is smaller than 5.444. As the same process as $n = 5$, the 6-order matrix will pass the consistency check when λ is smaller than 6.625.

B. Case study with one kind preference of five criteria

One kind important scale preference of the five criteria is set for case study in this section. The scenario of judgment is as follows: The government wants to enforce its homeland security using the WSN to aggregate the information on the borderline [22]. In such a scenario, the perimeter surveillance is one of the most promising WSN applications. WSN can be easily deployed permanently (e.g., public places) or on-demand (e.g., high risk events) in a very short time, low costs,

with little or no supporting communications infrastructure. As pair-wise comparison, the important scale of the 5 criteria can be decided: Scalability (1) < Key connectivity (3) < Storage overhead (5) < Resilience (7) < Communication overhead (9). In this inequality, higher value means higher important scale [3]. As both the judgment matrix (Matrix A) and the matrixes for KMs which respect to each criterion's comparison (Matrix B_S, B_K, B_R, B_M and B_C) are obtained, final vectors for each KM in the assumed WSN scenario are calculated. Recalling the overall weights, we can get a final value for each KM. The value for H. Chan *et al.* 2003 (H03) [7] is 0.175555. Similarly, the values for the other schemes in turns are calculated: L. Eschenauer *et al.* 2002 (L02) [16] = 0.270595; C. Blundo *et al.* 1992 (C92) [8] = 0.170659; S. Zhu *et al.* 2003 (Z03) [17] = 0.125337; M. Shehab *et al.* 2005 (M05) [18] = 0.124683; S. Slijepcevic *et al.* 2002 (S02) [19] = 0.129819. Comparing the final 6 value of the vectors, we get the biggest vector: L02 and the least vector: M05.

III. Our Proposal

In this section, we analyze characteristics of some KM schemes in WSN. Our analysis is based on the examination of corresponding evaluation criteria based on AHP-aided method [3]. In original AHP [4], the absolute number of important scale are definite. In our proposal, all important scale permutations of the corresponding evaluation criteria are presented. The all permutation of importance scale can help us to see all the cases results and get a overall conclusion.

A. Proposal description

The AHP-aided method and a corresponding case study have been introduced in section II. In that case study, only one kind preference of the criteria's importance scale is set. One kind of the preference of the criteria's importance scale can obtain one kind importance values of each criterion $A = (a_{ij})_{6\times6}$. One kind importance values of each criterion $A = (a_{ij})_{6\times6}$ can calculate one kind of the weighted vectors of the matrices $\overrightarrow{W}_A$. Because the weighted vectors of KMs $\overrightarrow{W}_B$ come from the importance values $B = (b_{mn})_{5\times5}$ and we know that $\overrightarrow{W}_k = \overrightarrow{W}_A \cdot \overrightarrow{W}_B$, the value of $\overrightarrow{W}_k$ will change as the value of $\overrightarrow{W}_A$.

There are different requirements of the importance scale among criteria under different parameters of network scenario. All permutations of the 5 criteria include 120-type situation. The affection of each criterion is analyzed. Then, we combined them together and analyze them synthetically.

For this target, we first provide an assumed WSN scenario and its corresponding parameters setting, especially the network size and its security requirement. One more network scenario for comparative analysis is followed. Comparing the two groups of network scenario, we get some generic conclusion among the 6 alternative KMs. Furthermore, we do experimental analysis among some more KMs. We choose 43 KMs [2] for comparison in our paper. These 43 KMs contain the currently mainly existed KMs. Based on these analysis, generic characters conclusion of these KMs are expected.

Our experiment has been executed on Toshiba Dynabook SS with a Core2, 1.40G CPU and 2048MB RAM memory. We implemented our experiment using the MATLAB. Each group of the experimental data has been calculated out within one minute.

B. Network scenario

In this section, we describe two groups of network scenarios: Network scenario A and Network scenario B.

Network Scenario A: We assume the network and key's parameters as follows: In each 1 km^2 square unit area, for providing available WSN model, we know that the relationship between communication distance l and limited power overhead E of each sensor node is $E \propto l^n$ $(2 < n < 4)$, n is effected by external influence and is usually set to 3 for calculation. Accordingly the communication radius of each node is set to 100 m [32]. Thus, the available nodes number is set to $N = 100$ for each 1 km^2 square unit area. Let p denote the probability of that two nodes share a key in pair-wise keys and let $d = p \times (N - 1)$ be the expected degree of a node. L02 [16] has shown that for a pool size $KP = 10,000$ keys, only 75 keys need to be stored in a node's memory to have the probability that they share a key in their key rings to be $p = 0.5$. Thus, the key pool size $KP = 10,000$ keys, the keys number 75 keys and the probability $p = 0.5$ which have been hold in scheme L02 [16] can be taken as an example here. At the key set up phase, each node ID is matched with Np other randomly selected nodes ID with probability $p = 0.5$ which are always used for a qualified value for evaluation [6]. Thus we can get $Np = 50$. At the beginning of the AHP evaluation, the matrix key distribution scheme generates an $m \times m$ key matrix for a WSN of size $N = m^2$. During the key pre-distribution phase, each node is assigned a position (i, j), receives both the keys in i-th column and the keys in j-th row of the key matrix as the key-chain, which total has $2m$ keys. Here m denotes the number of keys in master key list of a node and $m = \sqrt{N} = 10$. t is the size of group in assumed network scenario. $t = 100$ as if we assumes one group for the hierarchical structure here. Here $\lambda = 50$ is the size of adversary coalitions.

Network Scenario B: Scheme L02 [16] inferred that if the pool size is ten times larger, for example, $KP = 100,000$, then the number of keys required is still only 250 for keeping as the same $p = 0.5$ as in **Network Scenario A**. The basic scheme is a key management technique that is scalable, flexible and can also be used for large networks. Then we can present another WSN scenario based on it. We enlarge the key pool size and the network nodes number. The available nodes number is enlarged to $N = 1,000$. Because of the same probability $p = 0.5$, we obtain that $Np = 500$, $d = 500$, $t = 200$ (five groups for the hierarchical structure) and $m = 100$.

C. Criteria for KMs analysis in WSN

For the given quantitative comparisons and distinct assumptions made by these KMs, it may not be always possible to give

strict quantitative comparison criteria due to distinct assumptions made by these key management solutions. However, the following criteria can be used to evaluate and compare these key management schemes in WSN [3].

- Scalability (S): Ability of a key management solution to handle an increase in the WSN size.
- Key connectivity (K) : Probability that a pair or a group of sensor nodes can generate or find a common secret key to secure their communication.
- Resilience (R) : Resistance of the WSN against node capture.
- Storage overhead (M): Amount of memory units required to store security credentials.
- Processing overhead (P): Amount of processing cycles required by each sensor node to generate or find a common secret key.
- Communication overhead (C): Amount and size of messages exchanged between a pair or a group of sensor nodes to generate or find a common secret key.

Among the criteria, communication overhead is the amount and size of messages which are exchanged between a pair and a group of sensor nodes to generate or find a common secret key. Processing overhead is the amount of processing cycles required by each sensor node to generate or find a common secret key. Consider the power consumption [21], we can see that processing overhead is base on the hardware choosing and is not the main power consumption for WSN. Thus, processing overhead is not taken into evaluation in our evaluation method.

IV. Experimental analysis

A. Enumeration of all permutations for the importance scale of preference on the 5 criteria

One kind important scale preference of the five criteria is set for case study of six alternative KMs in the subsection *B* of the section II. If we did all permutation of the preference of the five criteria's importance scale, the number of cases are 120 in all. Under each case, there is different preference of the importance scale of each criterion.

For criterion S, K, R, M and C, there are different linear changes as increasing progressively or decreasing progressively by different unit cases. The different linear change and the different size of their unit cases maintain consistency with the experiments coding.

Under no affection of universality, we elaborate our all permutation by taking the preference importance scale of criterion scalability(S) as an example. Criterion S has the lowest preference in the first 25-case of the 120-case number (1-25 cases), the fourth preference in the second 25-case of the 120-case number (26-50 cases), the third preference in the third 25-case of the 120-case number (51-75 cases), the second preference in the fourth 25-case of the 120-case number (76-100 cases) and the highest preference in the last 20-case of the 120-case number (101-120 cases). The preference on S keeps in increase progressively as case number increasing by each unit-case. The last 20-case have the highest preference.

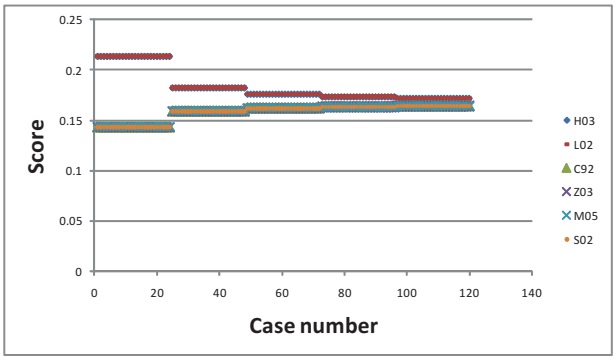


Fig. 3. Result of the optimum scheme in 120-case under one kind of criteria: Scalability

Its preference changing in each unit-case depends on the order of all criteria permutation.

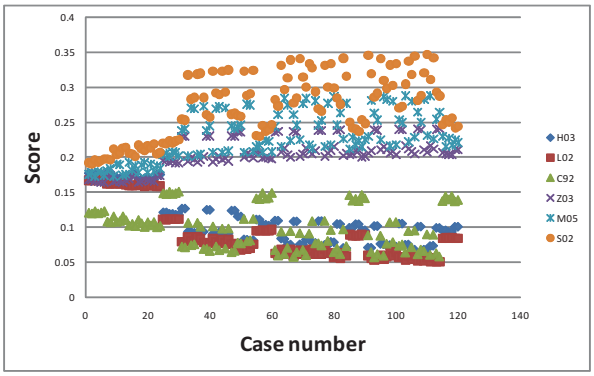
From Fig. 3, scheme H03 and scheme L02 have the same values and their values are always higher than the other four schemes as the preference changing of S. As the preference important scale of S becomes higher as the case number increasing, both scheme H03 and L02 lose their advantage gradually. This result shows that these two schemes have no obvious advantage on scalability. In Fig. 3, we obtain 120-case of the optimum scheme under enumeration of all the permutations of preference important scale on the S. In other words, these 120-case optimum schemes can be selected based on the other four criteria K, R, M and C, respectively.

B. Comparison of the 6 alternative KMs

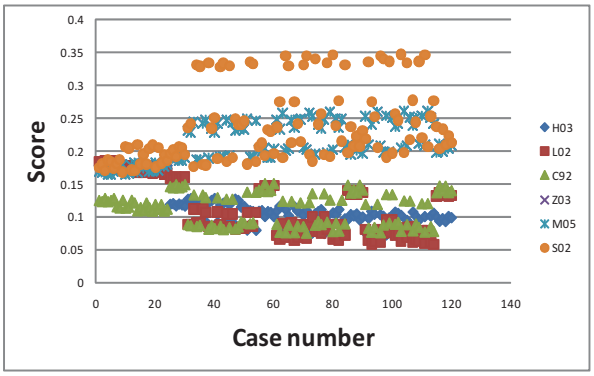
In this section, we synthesize the five criteria which are the integral requirement of the goal network scenario. We do all permutation of the five criteria for the same 6 alternative KMs (Scheme H03 [7], L02 [16], C92 [8], Z03 [17], M05 [18] and S02 [19]) which have been informed in section II. Two kinds of goal network scenarios: Network Scenario A and Network Scenario B are added not only for elaboration of all permutations but also for comparison among different scenarios. They are showed in Fig. 4.

From Fig. 4(a), the results show that L02 is better than Z03 and C92 in DWSN. S02 is better than Z03 and M05 in HWSN. The scores of KMs for DWSN are higher than KMs for HWSN. Especially, H03 scheme has higher score than other schemes except for L02 but never be the optimum one. Z03 scheme has most of the lowest score, but it has 4-type to be optimums. Fig. 4(a) shows the evaluation results of Network Scenario A while Fig. 4(b) shows Network Scenario B. There are some points and different points between Fig. 4(a) and Fig. 4(b).

- Same point 1: Scheme S02 takes most of the advantages under parameters 2 as shown in both Fig. 4(a) and Fig. 4(b). Scheme M05, C92, L02 and H03 don't change obviously in both parameter settings.
- Same point 2: In Fig. 4(a), all KMs in DWSN and HWSN have similar value in the first 25-case while similar



(a) Network Scenario A



(b) Network Scenario B

Fig. 4. Result of evaluation in 120-case under two kind parameters setting of WSN scenario

trend is shown in Fig. 4(b). This indicates there is not obvious affection of KMs selection for different network structures, as when scalability is not very important.

- Different point: We can see that scheme S02 does not keep the overwhelming advantage under the second group of parameters as under the first group. In other words, S02 scheme has more obvious advantage under small size network. The score of Z03 scheme reduces obviously under the second group of parameters compared to the first group.

C. Comparison among the 43 KMs

The **Table 4 Evaluation of the solution** in Camtepe et al. [2] shows 43 KMs in all, which covered almost current existed schemes. All schemes in that **Table 4** have been divided into seven groups. In each group, some schemes can be omitted by the others from the integral parameter values visibly. After that, there are 18 schemes left, which have complex values and cannot be compared directly. We divide the left 18 schemes into 3 groups according to the original orders. Firstly, we do the comparisons under the requirements of Network scenario A and get corresponding optimum scheme. Then we analysis the characteristics of the final optimum scheme.

- Multi IOS [23] is the optimum scheme of first group: All pair-wise(naive scheme), Matrix key [25], Closest pair-wise [22], IOS [23], Multiple IOS [23], PIKE [24].
- BROSK [26] is the optimum scheme of second group: BROSK [26], Polynomial based [8], Grid-group deployment [27], Pair-wise key establishment [28], Combinatorial-symmetric [29] and Combinatorial-hybrid [29].
- μ-TESLA extensions [31] is the optimum scheme of third group: Polynomial-non-interactive [8], HARPS [30], LEAP pair-wise [17], LEAP group-wise [17], Multi-tiered [19] and μ-TESLA extensions [31].

After got results from the three groups, the final comparison is among Multi IOS [23], BROSK [26] and μ-TESLA extensions [31]. The optimum scheme is the μ-TESLA extensions scheme [31].

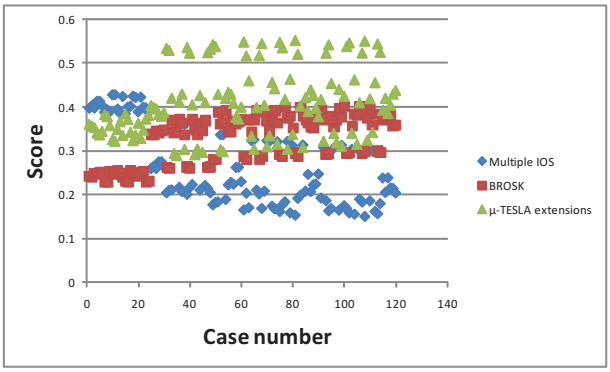


Fig. 5. Final evaluation result for optimum scheme selection among three KMs

In Fig. 5, μ-TESLA [31] scheme has an advantage over Multi IOS [23] and BROSK [26] in most cases. Because μ-TESLA [31] extensions can provide low overhead, tolerance of message loss, scalability to large networks and resistance to replay attacks as well as some known DOS attacks. These characteristics support the requirements of Network scenario A. On the contrary, μ-TESLA [31] will lose its advantages when both criteria K and R have not very high important scale. This character is also shown in Fig. 5 during the case number is in the near to 40, 80 and 100 respectively.

V. Conclusions

In this paper, we have presented performance analysis for key management scheme under assumed wireless sensor network scenario requirements. Our analysis is based on five criteria: scalability, key connectivity, resilience, storage overhead and communication overhead. We do all permutation of the five criteria for furthermore clarify. We first analyze the characteristics among six typical schemes. Furthermore, we do the analysis among almost all current existing schemes. Some interesting conclusions are presented during the analysis.

VI. Acknowledge

The first author is supported by the governmental scholarship from China Scholarship Council (CSC). The second author was supported by CSC.

References

[1] Y. Jeong, S. Lee, Hybrid Key Establishment Protocol Based on ECC for Wireless Sensor Network, in: *The 4th international conference on Ubiquitous Intelligence and Computing*, Volume 4611, pp.1233-1242, Hong Kong, China, 2007.

[2] S. A. CAMTEPE, B. Yener, Key management in wireless sensor network, in: *IOS Press*, 2008.

[3] R. Na, Y. Ren, Y. Hori, K. Sakurai, A Generic Evaluation Method for Key Management Schemes in Wireless Sensor Network, in: *Proc. of Int. Conf. on Ubiquitous Information Management and Communication (ACM ICUIMC 2011)*, 2011

[4] T. L. Saaty, *The Analytic Hierarchy Process*, in: McGraw-Hill, New York, 1980.

[5] J. Hwang, I. Syamsuddin, Information Security Policy Decision Making: An Analytic Hierarchy Process Approach, in: *2009 Third Asia International Conference on Modelling and Simulation*, pp.158-163, 2009.

[6] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, M. Galloway, A survey of key management schemes in wireless sensor networks, in: *Computer Communications*, 30, 2007, pp. 2314-2341.

[7] H.Chan, A Perrig, D. Song, Random key pre-distribution schemes for sensor networks, in: *IEEE Symp. Security and Privacy*, 2003, p.197.

[8] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, Perfectly-secure key distribution for dynamic conferences, in: *Crypto*, 1992.

[9] D. Chakrabarti, S. Maitra, B. Roy, A key pre-distribution scheme for wireless sensor networks: Merging blocks in combinatorial design, in: *Lecture notes in computer science*, ISSN 0302-9743.

[10] T. Ito, H Ohta, N Matsuda, T. Yoneda, A key pre-distribution scheme for secure sensor network using probability density function of node deployment, in: *Proceedings of the 3rd ACM*.

[11] L. Gong, D. J. Wheeler, A matrix key distribution schemes, in: *Journal of Cryptology*, 2(1) (1990) 51-59.

[12] B. Dutertre, S. Cheung, J. Levy, Lightweight key management in wireless sensor networks by leveraging initial trust, in: *Tech. Rep. SRI-SDL-04-02, System Design laboratory* (2004).

[13] C. Fei, Pair-wise Key Management in Wireless Sensor Network, in: *Computer Simulation[J]*, vol 22-5,2005.

[14] E. H. Forman, Decision by Objective, in: *http://mdm.gwu.edu/Forman/DBO.pdf*.

[15] *http://www.isc.senshu-u.ac.jp/ thc0456/EAHP/AHPweb.html*.

[16] L. Eschenauer, V. D. Gligor, A key-management scheme for distributed sensor networks, in: *ACM Conf. Computer and Commun. Security*, pp. 41-47, 2002.

[17] S. Zhu, S. Setia, S. Jajodia, Leap:Efficient security mechanisms for large-scale distirbuted sensor networks, in: *ACM Conf. Computer and Commun. Security*, pp. 62-72, 2003.

[18] M.Shehab, E.Bertino, A.Ghafoor, Efficient hierarchical key generation and key diffusion for distribution for distributed sensor networks, in: *IEEE Int. Conf. Sensor and Ad Hoc Commun. and Netw.*, pp. 76-84, 2005.

[19] S.Slijepcevic, M.Potkonjak, V.Tsiatsis, S.Zimbeck, M.B.Srivastava, On communication security in wireless ad-hoc sensor network, in: *IEEE WETICE*, pp. 139-144, 2002.

[20] A. Casaca, D. Westhoff, Scenario Definition and Initial Threat Analysis, in: *UbiSec and Sens Deliverable D0.1*, 2006

[21] M. Gabriela, C. Torres, Enegry Consumption in wireless sensor network using GSP, in: *Thesis for master degree,University of Pittsburgh*, 2006

[22] D. Liu, P. Ning, Location based pairwise key establishment for static sensor networks, in: *ACM Workshop on Security of Ad Hoc and Sensor Netw.*, 2003.

[23] J. Lee, D. R. Stinson, Deterministic key pre-distribution schemes for distributed sensor networks, in: *ACM Symp. Applied Computing*, 2005.

[24] H. Chan, A. Perrig, Pike: Peer intermediaries for key establishment, in: *IEEE INFOCOM*, 2005.

[25] L. Gong, D. J. Wheeler, A matrix key distribution scheme, in: *Journal of Cryptology 2(1)*,1990.

[26] B. Lai, S. Kim, I. Verbauwhede, Scalable session key construction protocol for wireless sensor networks, in: *IEEE Workshop on Large Scale Real-Time and Embedded Systems*, 2002.

[27] D. Huang, M. Mehta, D. Medhi, L. Harn, Location-aware key management scheme for wireless sensor networks, in: *ACM Workshop on Security of Ad Hoc and Sensor Netw.*, 2004.

[28] S. Zhu, S. Xu, S. Setia, S. Jajodia, Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach, in: *IEEE Int. Conf. Netw. Protocols*, 2003.

[29] S. A. Camtepe, B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks, in: *ESORICS*, 2004.

[30] M. Ramkumar, N. Memon, An efficient random key pre-distribution scheme, in: *IEEE Global Telecommunications Conference*, 2004.

[31] D. Liu, P. Ning, Multi-level μ-tesla: A broadcast authentication system for distributed sensor networks, in: *Tech. Rep. TR-2003-08*, Department of Computer Science, North Carolina State University, 2003.

[32] G. Zhou, Z. Zhu, G. Chen, N. Hu, Energy-Effcient Chain-Type Wireless Sensor Network for Gas Monitoring, in: *Proceeding of The Second International Conference on Information and Computing Science*, pp. 125-128, May, 2009